

# Orders of Tate-Shafarevich groups for the Neumann-Setzer type elliptic curves

Andrzej Dąbrowski and Lucjan Szymaszkiewicz

*Abstract.* We present the results of our search for the orders of Tate-Shafarevich groups for the Neumann-Setzer type elliptic curves.

Key words: elliptic curves, Tate-Shafarevich group, Cohen-Lenstra heuristics, distribution of central  $L$ -values

2010 Mathematics Subject Classification: 11G05, 11G40, 11Y50

## 1 Introduction

Let  $E$  be an elliptic curve defined over  $\mathbb{Q}$  of conductor  $N_E$ , and let  $L(E, s)$  denote its  $L$ -series. Let  $\mathfrak{W}(E)$  be the Tate-Shafarevich group of  $E$ ,  $E(\mathbb{Q})$  the group of rational points, and  $R(E)$  the regulator, with respect to the Néron-Tate height pairing. Finally, let  $\Omega_E$  be the least positive real period of the Néron differential on  $E$ , and define  $C_\infty(E) = \Omega_E$  or  $2\Omega_E$  according as  $E(\mathbb{R})$  is connected or not, and let  $C_{\text{fin}}(E)$  denote the product of the Tamagawa factors of  $E$  at the bad primes. The Euler product defining  $L(E, s)$  converges for  $\text{Re } s > 3/2$ . The modularity conjecture, proven by Wiles-Taylor-Diamond-Breuil-Conrad, implies that  $L(E, s)$  has an analytic continuation to an entire function. The Birch and Swinnerton-Dyer conjecture relates the arithmetic data of  $E$  to the behaviour of  $L(E, s)$  at  $s = 1$ .

Let  $g_E$  be the rank of  $E(\mathbb{Q})$  and let  $r_E$  denote the order of the zero of  $L(E, s)$  at  $s = 1$ .

**Conjecture 1** (*Birch and Swinnerton-Dyer*) (i) We have  $r_E = g_E$ ,  
(ii) the group  $\mathfrak{W}(E)$  is finite, and

$$\lim_{s \rightarrow 1} \frac{L(E, s)}{(s - 1)^{r_E}} = \frac{C_\infty(E) C_{\text{fin}}(E) R(E) |\mathfrak{W}(E)|}{|E(\mathbb{Q})_{\text{tors}}|^2}.$$

If  $\mathfrak{W}(E)$  is finite, the work of Cassels and Tate shows that its order must be a square.

The first general result in the direction of this conjecture was proven for elliptic curves  $E$  with complex multiplication by Coates and Wiles in 1976 [4], who showed that if  $L(E, 1) \neq 0$ , then the group  $E(\mathbb{Q})$  is finite. Gross and Zagier [17] showed that if  $L(E, s)$  has a first-order zero at  $s = 1$ , then  $E$  has a rational point of infinite order. Rubin [25] proves that if  $E$  has complex multiplication and  $L(E, 1) \neq 0$ , then  $\mathfrak{W}(E)$  is finite. Kolyvagin [19] proved that, if  $r_E \leq 1$ , then  $r_E = g_E$  and  $\mathfrak{W}(E)$  is finite. Very recently, Bhargava, Skinner and Zhang [1] proved that at least 66.48% of all elliptic curves over  $\mathbb{Q}$ , when ordered by height, satisfy the weak form of the Birch and Swinnerton-Dyer conjecture, and have finite Tate-Shafarevich group.

Coates et al. [3] [2], and Gonzalez-Avilés [16] showed that there is a large class of explicit quadratic twists of  $X_0(49)$  whose complex  $L$ -series does not vanish at  $s = 1$ , and for which the full Birch and Swinnerton-Dyer conjecture is valid. The deep results by Skinner-Urban [30] allow (in practice, see section 3 for instance) to establish the full version of the Birch and Swinnerton-Dyer conjecture for a large class of elliptic curves without CM.

The numerical studies and conjectures by Conrey-Keating-Rubinstein-Snaith [6], Delaunay [11][12], Watkins [33], Radziwiłł-Soundararajan [24] (see also the papers [9] [7] [8] and references therein) substantially extend the systematic tables given by Cremona.

Given an integer  $u \equiv 1 \pmod{4}$ , such that  $u^2 + 64$  is square-free, we define two families of elliptic curves of conductor  $u^2 + 64$  (we call them the *Neumann-Setzer type elliptic curves*):

$$E_1(u) : \quad y^2 + xy = x^3 + \frac{1}{4}(u-1)x^2 - x,$$

and

$$E_2(u) : \quad y^2 + xy = x^3 + \frac{1}{4}(u-1)x^2 + 4x + u.$$

In this paper we present the results of our search for the orders of Tate-Shafarevich groups for the Neumann-Setzer type elliptic curves. Our data contains values of  $|\mathfrak{W}(E_i(u))|$  for 2056445 values of  $u \equiv 1 \pmod{4}$ ,  $|u| \leq 10^7$  such that  $u^2 + 64$  is a product of odd number of different primes, and such that  $L(E(u), 1) \neq 0$  (456702 of these values satisfy the condition  $u^2 + 64$  is a prime). Additionally, we have considered 10000 values of  $u \equiv 1 \pmod{4}$ ,  $|u| \geq 10^8$  such that  $u^2 + 64$  is a product of odd number of different primes, and in cases  $L(E(u), 1) \neq 0$  we computed the orders of  $\mathfrak{W}(E_i(u))$ . Our data extends the calculations given by Stein-Watkins [32] (resp. by Delaunay-Wuthrich [15]), where the authors considered  $|u| \leq \sqrt{2} \times 10^6$  (resp.  $|u| \leq 10^6$ ) such that  $u^2 + 64$  is a prime.

Our main observations concern the asymptotic formulae in sections 4 (frequency of orders of  $\mathbb{W}$ ) and 6 (asymptotics for the sums  $\sum |\mathbb{W}(E_i(u))| R(E_i(u))$  in the rank zero and one cases), and the distributions of  $\log L(E_i(u), 1)$  and  $\log(|\mathbb{W}(E_i(u))|/\sqrt{|u|})$  in section 7.

We thank Bjorn Poonen and Christophe Delaunay for their remarks and questions. We thank the anonymous referee for his/her remarks and comments which improved the final version of this paper.

Our experimental data were obtained using the the PARI/GP software [23]. The computations were carried out in 2015 and 2016 on the HPC cluster HAL9000 and desktop computers Core(TM) 2 Quad Q8300 4GB/8GB. All machines are located at the Department of Mathematics and Physics of Szczecin University.

## 2 Preliminaries

We have  $\Delta_{E_1(u)} = u^2 + 64$ , and  $\Delta_{E_2(u)} = -(u^2 + 64)^2$ . The curves  $E_1(u)$  and  $E_2(u)$  are 2-isogenous: write  $E_1(u)$  and  $E_2(u)$  in short Weierstrass forms ( $y^2 = x^3 + ux^2 - 16x$  and  $y^2 = x^3 - 2ux^2 + (u^2 + 64)x$ , respectively), and use ([29], Example 4.5 on p. 70). It is known, due to Neumann and Setzer ([21], [28]), that in the case  $u^2 + 64$  is a prime, the curves  $E_1(u)$  and  $E_2(u)$  are the only (up to isomorphism) elliptic curves with a rational 2-division point and conductor  $u^2 + 64$ . In general there are more than two, up to isomorphism, elliptic curves with a rational 2-division point and conductor  $u^2 + 64$ . Take, for instance,  $u = -51$ , then the curves  $E_1(u)$  and  $E_2(u)$  have conductor  $2665 = 5 \cdot 13 \cdot 41$ . In Cremona's online tables we find 8 elliptic curves of conductor 2665 with a rational 2-division point.

**Lemma 1** *We have (i)  $E_1(u)(\mathbb{Q})_{tors} \simeq E_2(u)(\mathbb{Q})_{tors} \simeq \mathbb{Z}/2\mathbb{Z}$ ; (ii)  $\Omega_{E_1(u)} = \Omega_{E_2(u)}$ ,  $C_\infty(E_1(u)) = 2\Omega_{E_1(u)}$ ,  $C_\infty(E_2(u)) = \Omega_{E_2(u)}$ ; (iii)  $C_{fin}(E_1(u)) = 1$ , and  $C_{fin}(E_2(u)) = 2^k$ , where  $u^2 + 64 = p_1 \cdots p_k$ .*

*Proof.* (i) Let  $E(u) = E_1(u)$  or  $E_2(u)$ . Then  $E(u)$  has good reduction at 2. Using the reduction map modulo 2, we obtain that  $|E_i(u)(\mathbb{Q})_{tors}|$  divides 4. Now, one checks that  $E_i(u)(\mathbb{Q})$  have only one point of order two, and no points of order four. (ii) To check that  $\Omega_{E_1(u)} = \Omega_{E_2(u)}$ , one uses the explicit forms of Weierstrass equations. Now the sign of the discriminant of  $E_1(u)$  (resp. of  $E_2(u)$ ) is positive (resp. negative), hence the remaining assertions follow. (iii) We have  $C_{fin}(E_1(u)) = \prod_{p|\Delta_{E(u)}} C_p(E(u))$ , where  $C_p(E(u)) = [E(u)(\mathbb{Q}_p) : E_0(u)(\mathbb{Q}_p)]$ , and  $E_0(u)(\mathbb{Q}_p)$  denotes the subgroup of

points of  $E(u)(\mathbb{Q}_p)$  with non-singular reduction modulo  $p$ . Both  $E_1(u)$  and  $E_2(u)$  have split multiplicative reductions at all primes  $p$  dividing  $u^2 + 64$ . Hence, in this case,  $C_p(E(u)) = \text{ord}_p(\Delta_{E(u)})$  (see, for instance, [2], Lemma 2.9), and the assertion follows.

Note that  $L(E_1(u), s) = L(E_2(u), s) = \sum_{n=1}^{\infty} a_n n^{-s}$ ,  $\text{Re}(s) > 3/2$ . Assuming the truth of the Birch and Swinnerton-Dyer conjecture for  $E(u)$  in the rank zero case, we can calculate the order of  $\mathbb{W}(E(u))$  by evaluating (an analytic continuation of)  $L(E(u), s)$  at  $s = 1$ :

$$|\mathbb{W}(E_1(u))| = \frac{2L(E_1(u), 1)}{\Omega_{E_1(u)}},$$

$$|\mathbb{W}(E_2(u))| = \frac{L(E_2(u), 1)}{2^{k-2}\Omega_{E_2(u)}},$$

where as above,  $u^2 + 64 = p_1 \cdots p_k$  is a product of different primes.

More precisely, we have to calculate the value

$$L(E(u), 1) = 2 \sum_{n=1}^{\infty} \frac{a_n}{n} e^{-\frac{2\pi n}{\sqrt{u^2+64}}}$$

with sufficiently accuracy.

**Lemma 2** *In order to determine the order of  $\mathbb{W}(E_1(u))$  and  $\mathbb{W}(E_2(u))$ , it is enough to take  $\frac{1}{8}\sqrt{u^2 + 64} \log(u^2 + 64)$  terms of the above series.*

*Proof.* Repeat the proof of Theorem 16 in [15].

Let  $\epsilon(E(u))$  denote the root number of  $E(u)$ .

**Lemma 3** *Let  $u^2 + 64 = p_1 \cdots p_k$  be a product of different primes. Then  $\epsilon(E(u)) = (-1)^{k+1}$ .*

*Proof.*  $\epsilon(E(u)) = -\prod_{i=1}^k \epsilon_{p_i}(E(u))$ , a product of local root numbers. Now,  $E(u)$  has split multiplicative reduction at all  $p_i$  dividing  $u^2 + 64$ . Hence,  $\epsilon_{p_i}(E(u)) = -1$ , and the assertion follows.

**Corollary 1** *Assume the parity conjecture holds for the curves  $E(u)$ . Then  $E(u)(\mathbb{Q})$  has even rank if and only if  $u^2 + 64 = p_1 \cdots p_k$  is a product of odd number of different primes.*

We can use a classical 2-descent method ([29], Chapter X) to obtain a bound on the rank of  $E_i(u)$  depending on  $k$ . Let  $\phi : E_1(u) \rightarrow E_2(u)$  be the 2-isogeny, and write  $\hat{\phi}$  for its dual. Let  $S^{(\phi)}$  and  $S^{(\hat{\phi})}$  denote the corresponding Selmer groups. One checks that  $S^{(\phi)} \subset \langle p_1, \dots, p_k \rangle$  and  $S^{(\hat{\phi})} = \langle -1 \rangle$ . As a consequence, we obtain  $\text{rank}(E_i(u)) \leq \dim_{\mathbb{F}_2} S^{(\phi)} + \dim_{\mathbb{F}_2} S^{(\hat{\phi})} - 2 \leq k + 1 - 2 = k - 1$ . In particular, if  $u^2 + 64$  is a prime, then  $E_i(u)$  have rank zero, and if  $k = 2$ , then  $\text{rank}(E_i(u)) \leq 1$  ( $= 1$  if we assume the parity conjecture).

**Definition 2** *We say that an integer  $u \equiv 1 \pmod{4}$  satisfies condition (\*), if  $u^2 + 64$  is a prime; we say that an integer  $u \equiv 1 \pmod{4}$  satisfies condition (\*\*), if  $u^2 + 64$  is a product of odd number of different primes.*

### 3 Birch and Swinnerton-Dyer conjectur for Neumann-Setzer type elliptic curves

In this section, we will use the deep results by Skinner-Urban [30] (and other available techniques), to prove the full version of the Birch-Swinnerton-Dyer conjecture for a large class of Neumann-Setzer type elliptic curves.

Let  $\bar{\rho}_{E,p} : \text{Gal}(\mathbb{Q}/\mathbb{Q}) \rightarrow \text{GL}_2(\mathbb{F}_p)$  denote the Galois representation on the  $p$ -torsion of  $E$ . Assume  $p \geq 3$ .

**Theorem 3** ([30], Theorem 2) *Let  $E$  be an elliptic curve over  $\mathbb{Q}$  with conductor  $N_E$ . Suppose: (i)  $E$  has good ordinary reduction at  $p$ ; (ii)  $\bar{\rho}_{E,p}$  is irreducible; (iii) there exists a prime  $q \neq p$  such that  $q \parallel N_E$  and  $\bar{\rho}_{E,p}$  is ramified at  $q$ ; (iv)  $\bar{\rho}_{E,p}$  is surjective. If moreover  $L(E, 1) \neq 0$ , then the  $p$ -part of the Birch and Swinnerton-Dyer conjecture holds true, and we have*

$$\text{ord}_p(|\mathfrak{W}(E)|) = \text{ord}_p \left( \frac{|E(\mathbb{Q})_{\text{tors}}|^2 L(E, 1)}{C_{\infty}(E) C_{\text{fin}}(E)} \right).$$

Take  $E(u) = E_1(u)$  or  $E_2(u)$ . Then:

a)  $E(u)$  is semistable and has a rational 2-division point, hence  $\bar{\rho}_{E(u),p}$  is irreducible for  $p \geq 7$  by ([10], Theorem 7). Note moreover (by Wiles [34]) that at least one of  $\bar{\rho}_{E(u),3}$  or  $\bar{\rho}_{E(u),5}$  is irreducible.

b) If  $E$  is any semistable elliptic curve and  $q \neq p$ , then  $\bar{\rho}_{E,p}$  is unramified at  $q$  if and only if  $p \mid \text{ord}_q(\Delta_E)$ . In our case,  $\text{ord}_q(\Delta_E(u))$  equals 1 or 2, hence  $\bar{\rho}_{E(u),p}$  is ramified at any  $q \geq 3$ .

c) If  $E$  is any semistable elliptic curve, then  $\bar{\rho}_{E,p}$  is surjective for  $p \geq 11$  by [27]. More precisely, Serre ([27], Prop. 1) shows that in this case  $\bar{\rho}_{E,p}$

is surjective for all primes  $p$  unless  $E$  admits an isogeny of degree  $p$  defined over  $\mathbb{Q}$ . In particular, if such  $E$  additionally has a rational 2-division point, then  $\bar{\rho}_{E,p}$  is surjective for  $p \geq 7$ . Note (by [26], Prop. 21, and [27], Prop. 1), that in the case of semistable elliptic curve  $E$ , the representation  $\bar{\rho}_{E,p}$  is surjective if and only if it is irreducible. Now, Zywina ([35], Prop. 6.1) gives a criterion to determine whether  $\bar{\rho}_{E,p}$  is surjective or not for any non-CM elliptic curve and any prime  $p \leq 11$ . Using such a criterion, one immediately checks surjectivity of  $\bar{\rho}_{E_i(u),p}$  for  $p = 2, 3$ , and  $5$ . As a consequence, we obtain the following general result.

**Proposition 1** *The representations  $\bar{\rho}_{E(u),p}$  are surjective for all primes  $p$ .*

Summing up all the above information, we obtain the following nice result.

**Corollary 2** *Let  $E = E_1(u)$  or  $E_2(u)$ , with  $u \equiv 1 \pmod{4}$  satisfying (\*\*) and such that  $L(E, 1) \neq 0$ . If  $E$  has good ordinary reduction at  $p \geq 3$ , then the  $p$ -part of the Birch and Swinnerton-Dyer conjecture holds for  $E$ .*

**Remark.** Let us recall that a prime  $p$  is *good* for an elliptic curve  $E$  over  $\mathbb{Q}$ , if  $p$  does not divide  $N_E$ ;  $p$  is *good ordinary* for  $E$ , if is good and  $a_p = p + 1 - N_p(E)$  is not divisible by  $p$  (here  $N_p(E)$  denotes the number of  $\mathbb{F}_p$ -points of the reduction  $E_p$ ). Here are explicit conditions for small primes  $p$  to satisfy the good ordinary condition in case  $E = E_i(u)$  (we assume  $u \equiv 1 \pmod{4}$ ): (i)  $p = 3$ , additional condition  $u \not\equiv 0 \pmod{3}$ ; (ii)  $p = 5$ , no additional condition on  $u$ ; (iii)  $p = 7$ , additional condition  $u \not\equiv 0 \pmod{7}$ ; (iv)  $p = 11$ , additional condition  $u \not\equiv 0, 4, 7 \pmod{11}$ .

**Remark.** One can use explicit descent algorithms to compute  $\mathbb{W}(E_i(u))[m]$  for  $m = 2, 4$  or  $8$ . If  $\mathbb{W}(E_i(u))[2]$  is trivial, then  $\mathbb{W}(E_i(u))$  has odd order. If  $\mathbb{W}(E_i(u))[2] = \mathbb{W}(E_i(u))[4]$ , say, then  $\text{ord}_2|\mathbb{W}(E_i(u))| = \text{ord}_2|\mathbb{W}(E_i(u))[2]|$ . Similarly, one can use explicit descent algorithms to compute  $\mathbb{W}(E_i(u))[m]$  for  $m = 3$  or  $9$ . Again, if  $\mathbb{W}(E_i(u))[3]$  is trivial, then  $\mathbb{W}(E_i(u))$  has order not divisible by  $3$  (here we not require that  $3$  is good ordinary). If  $\mathbb{W}(E_i(u))[3] = \mathbb{W}(E_i(u))[9]$ , then  $\text{ord}_3|\mathbb{W}(E_i(u))| = \text{ord}_3|\mathbb{W}(E_i(u))[3]|$ .

The theses [20] [31] explore both theoretical and computational methods to compute the orders of Tate-Shafarevich groups.

**Remark.** (i) Among 456702 values of  $u \equiv 1 \pmod{4}$ ,  $|u| \leq 10^7$  satisfying (\*), there are 379898 values of  $|u|$  such that  $E(u)$  has good ordinary reduction at any prime dividing the analytic order  $|\mathbb{W}(E(u))|$ . The groups  $\mathbb{W}(E_i(u))[2]$  are both trivial (by 2-descent), hence by Corollary 2 the values  $|\mathbb{W}(E(u))|$  are the algebraic orders of  $\mathbb{W}$ . (ii) Among 2056445 values of  $u \equiv 1 \pmod{4}$ ,  $|u| \leq 10^7$

satisfying (\*\*) and such that  $L(E(u), 1) \neq 0$ , there are 1148683 values of  $|u|$  such that  $|\mathbb{W}(E_2(u))|$  is odd and  $E(u)$  has good ordinary reduction at any prime dividing the analytic order  $|\mathbb{W}(E_2(u))|$ . Again, by Corollary 2 all these values are the algebraic orders of  $\mathbb{W}$ .

The numerical data are done under the Birch and Swinnerton-Dyer conjecture. In particular, the experimental study in sections 4, 5, 6, and 7 concern the analytic orders of the Tate-Shafarevich groups.

## 4 Frequency of orders of $\mathbb{W}$

Our calculations strongly suggest that for any positive integer  $k$  there are infinitely many integers  $u \equiv 1 \pmod{4}$  satisfying condition (\*\*), such that  $E(u)$  has rank zero and  $|\mathbb{W}(E(u))| = k^2$ . Below (end of this section) we will state a more precise conjecture.

Let  $f(i, X)$  denote the number of integers  $u \equiv 1 \pmod{4}$ ,  $|u| \leq X$ , satisfying (\*\*) and such that  $L(E(u), 1) \neq 0$ ,  $|\mathbb{W}(E_i(u))| = 1$ . Let  $g(X)$  denote the number of integers  $u \equiv 1 \pmod{4}$ ,  $|u| \leq X$ , satisfying (\*\*) and such that  $L(E(u), 1) = 0$ . We obtain the following graphs (compare [7] [8], where similar observations are made for the families of quadratic twists of several elliptic curves).

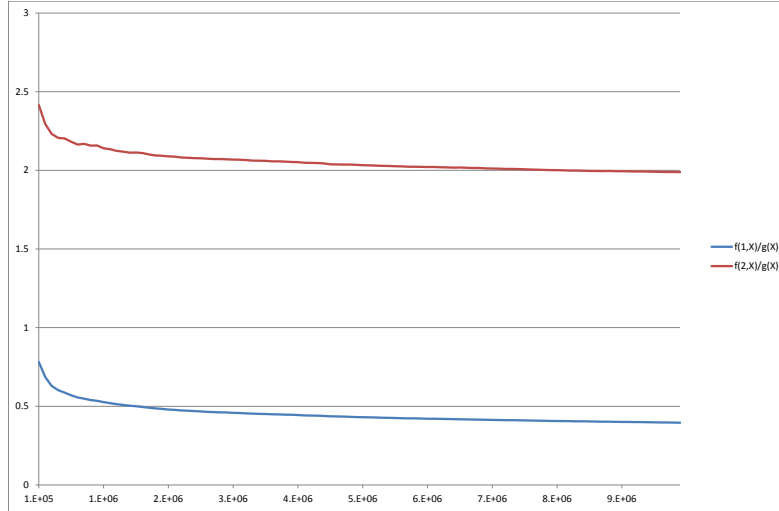


Figure 1: Graphs of the functions  $f(i, X)/g(X)$ ,  $i = 1, 2$ .

Consider the set consisting of 10000 values of integers  $u \equiv 1 \pmod{4}$ ,  $|u| \geq 10^8$ , satisfying (\*\*). Let  $f(i)$  denote the number of such  $u$ 's satisfying

$L(E_i(u), 1) \neq 0$  and  $|\mathbb{W}(E_i(u))| = 1$ , and let  $g$  denote the number of such  $u$ 's satisfying  $L(E_i(u), 1) = 0$ . Then  $f(1) = 118$ ,  $f(2) = 845$ ,  $g = 482$ , hence  $f(1)/g \approx 0,2448$ , and  $f(2)/g \approx 1,7531$ .

Delaunay and Watkins expect [14], Heuristics 1.1):

$$\#\{d \leq X : \epsilon(E_d) = 1, \text{rank}(E_d) \geq 2\} \sim c_E X^{3/4} (\log X)^{b_E + \frac{3}{8}}, \quad \text{as } X \rightarrow \infty,$$

where  $c_E > 0$ , and there are four different possibilities for  $b_E$ , largery dependent on the rational 2-torsion structure of  $E$ . Watkins [33], and Park-Poonen-Voight-Wood [22] have conjectured that

$$\#\{E : \text{ht}(E) \leq X, \epsilon(E) = 1, \text{rank}(E) \geq 2\} \sim cX^{19/24} (\log X)^{3/8},$$

where  $E$  runs over all elliptic curves defined over the rationals, and  $\text{ht}(E)$  denotes the height of  $E$ .

We expect a similar asymptotic formula for the family  $E(u)$ . Let  $H(X) := \frac{X^{19/24} (\log X)^{3/8}}{g(X)}$ , and  $G_i(X) := \frac{X^{3/4} (\log X)^i}{g(X)}$ ,  $i = 0, 1/2$  or  $1$ . We obtain the following graphs, (partially) confirming our expectation.

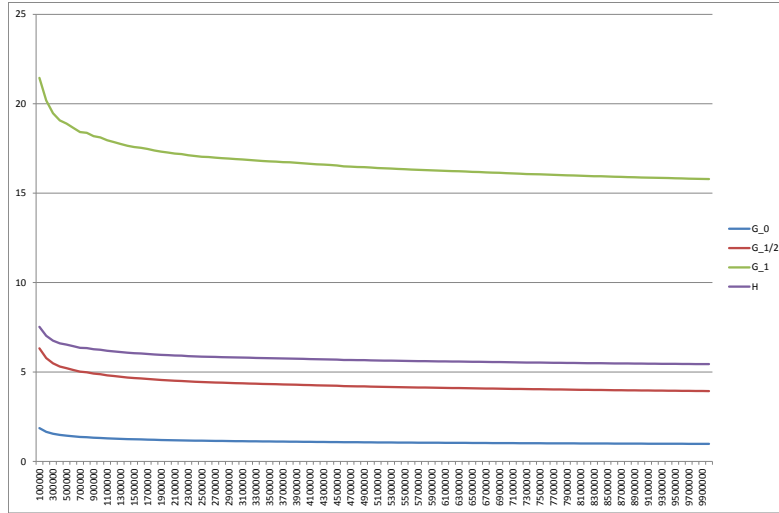


Figure 2: Graph of the function  $H(X)$ .

Now let  $f_k(i, X)$  denote the number of integers  $u \equiv 1 \pmod{4}$ ,  $|u| \leq X$ , satisfying  $(**)$  and such that  $L(E(u), 1) \neq 0$ ,  $|\mathbb{W}(E_i(u))| = k^2$ . Let  $F_k(i, X) := \frac{f(i, X)}{f_k(i, X)}$ . We obtain the following graphs of the functions  $F_k(i, X)$  for  $i = 1, 2$  and  $k = 2, 3, 4, 5, 6, 7$ .



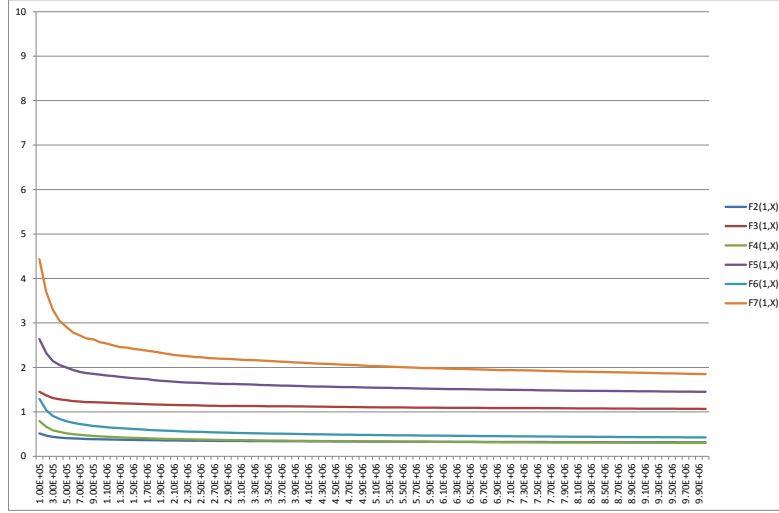


Figure 3: Graphs of the functions  $F_k(1, X)$ ,  $k = 2, \dots, 7$ .

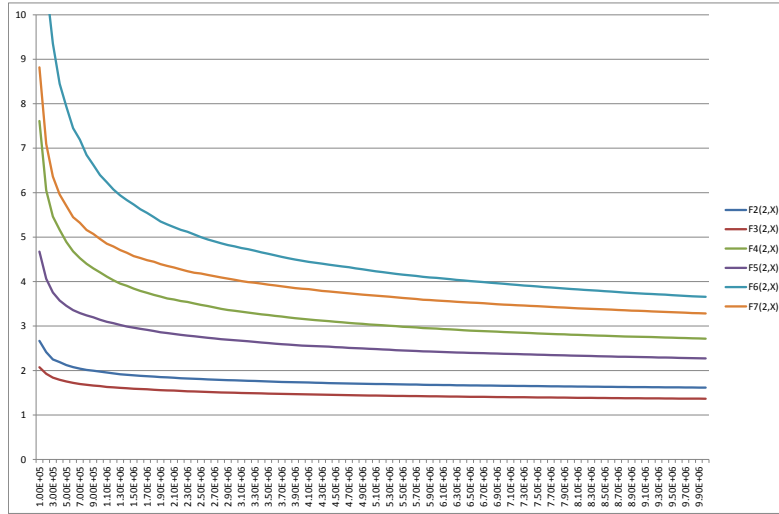


Figure 4: Graphs of the functions  $F_k(2, X)$ ,  $k = 2, \dots, 7$ .

The above calculations suggest the following

**Conjecture 4** *For any positive integer  $k$  there are constants  $c_{k,i} > 0$ ,  $\alpha_{k,i}$ , and  $\beta_{k,i}$  such that*

$$f_k(i, X) \sim c_{k,i} X^{\alpha_{k,i}} (\log X)^{\beta_{k,i}}, \quad \text{as } X \rightarrow \infty.$$

Conjectures 8 in [7] and 2 in [8] suggest similar asymptotics for the family of quadratic twists of any elliptic curve defined over  $\mathbb{Q}$ .

Consider the set consisting of 10000 values of integers  $u \equiv 1(\text{mod } 4)$ ,  $|u| \geq 10^8$ , satisfying (\*\*). Let  $f_k(i)$  denote the number of such  $u$ 's satisfying  $L(E_i(u), 1) \neq 0$  and  $|\mathbb{W}(E_i(u))| = k^2$ . Let  $F_k(i) := \frac{f_1(i)}{f_k(i)}$ . We obtain

$$\begin{aligned} F_2(1) &\approx 0.2256, & F_3(1) &\approx 0.8251, & F_4(1) &\approx 0.1779 \\ F_5(1) &\approx 1.0825, & F_6(1) &\approx 0.2494, & F_7(1) &\approx 1.1919 \\ F_2(2) &\approx 1.1901, & F_3(2) &\approx 1.0682, & F_4(2) &\approx 1.5590 \\ F_5(2) &\approx 1.4955, & F_6(2) &\approx 1.9031, & F_7(2) &\approx 1.8449 \end{aligned}$$

## 5 Cohen-Lenstra heuristics for the order of $\mathbb{W}$

Delaunay [12] has considered Cohen-Lenstra heuristics for the order of Tate-Shafarevich group. He predicts, among others, that in the rank zero case, the probability that  $|\mathbb{W}(E)|$  of a given elliptic curve  $E$  over  $\mathbb{Q}$  is divisible by a prime  $p$  should be  $f_0(p) := 1 - \prod_{j=1}^{\infty} (1 - p^{1-2j}) = \frac{1}{p} + \frac{1}{p^3} + \dots$ . Hence,  $f_0(2) \approx 0.580577$ ,  $f_0(3) \approx 0.360995$ ,  $f_0(5) \approx 0.206660$ ,  $f_0(7) \approx 0.145408$ ,  $f_0(11) \approx 0.092$ , and so on.

Let  $F(X)$  (resp.  $G(X)$ ) denote the number of integers  $u \equiv 1(\text{mod } 4)$ ,  $|u| \leq X$ , satisfying (\*) (resp. (\*\*)) and such that  $L(E(u), 1) \neq 0$ . Let  $F_p(X)$  (resp.  $G_p(X)$  if  $p \geq 3$ ) denote the number of integers  $u \equiv 1(\text{mod } 4)$ ,  $|u| \leq X$ , satisfying (\*) (resp. (\*\*)), such that  $L(E(u), 1) \neq 0$  and  $|\mathbb{W}(E(u))|$  is divisible by  $p$ . Let  $G_2(i, X)$  denote the number of integers  $u \equiv 1(\text{mod } 4)$ ,  $|u| \leq X$ , satisfying (\*\*), such that  $L(E(u), 1) \neq 0$  and  $|\mathbb{W}(E_i(u))|$  is divisible by 2. Let  $f_p(X) := \frac{F_p(X)}{F(X)}$ ,  $g_p(X) := \frac{G_p(X)}{G(X)}$ , and  $g_2(i, X) := \frac{G_2(i, X)}{G(X)}$ . We obtain the following tables, extending the calculations given by Stein-Watkins [32] and Delaunay-Wuthrich [15].

$X$	$f_3(X)$	$f_5(X)$	$f_7(X)$	$f_{11}(X)$
$2 \cdot 10^6$	0.358355	0.189909	0.123182	0.061527
$4 \cdot 10^6$	0.362001	0.192343	0.126864	0.066945
$6 \cdot 10^6$	0.363294	0.194413	0.129213	0.069780
$8 \cdot 10^6$	0.364051	0.196239	0.130556	0.071144
$10^7$	0.365067	0.197048	0.131812	0.072358

The numerical values of  $f_3(X)$  exceed the expected value  $f_0(3)$ . In general, the values  $f_k(X)$  may tend to some constants depending on the various congruential values of  $u$  (compare [32]).

It seems that it would be better to consider  $u$ 's satisfying (\*\*), but here the convergence is very slow. Here are the results.

$X$	$g_2(1, X)$	$g_2(2, X)$	$g_3(X)$	$g_5(X)$	$g_7(X)$	$g_{11}(X)$
$2 \cdot 10^6$	0.746231	0.313111	0.295592	0.127626	0.072959	0.030979
$4 \cdot 10^6$	0.761104	0.326554	0.303529	0.134259	0.078513	0.034796
$6 \cdot 10^6$	0.768805	0.333854	0.307670	0.138168	0.081543	0.036884
$8 \cdot 10^6$	0.774040	0.338854	0.310603	0.140959	0.083638	0.038350
$10^7$	0.777917	0.342322	0.312758	0.143060	0.085332	0.039481

Note that the value  $(g_2(1, 10^7) + g_2(2, 10^7))/2 \approx 0.56012$  is not so far from the expected one.

We have computed the orders of 9518 pairs of Tate-Shafarevich groups  $(\mathbb{W}(E_1(u)), \mathbb{W}(E_2(u)))$  for  $|u| \geq 10^8$ ,  $u \equiv 1 \pmod{4}$ , satisfying  $(*)$ , and such that  $L(E(u), 1) \neq 0$ . We obtained the following table.

$p$	2	3	5	7	11
Frequency of $p \mid  \mathbb{W}(E_1(u)) $	0.826329	0.332213	0.167262	0.111053	0.058100
Frequency of $p \mid  \mathbb{W}(E_2(u)) $	0.393045	0.332213	0.167262	0.111053	0.058100

## 6 Asymptotic formulae

### 6.1 The rank zero case

Let  $M^*(T) := \frac{1}{T^*} \sum |\mathbb{W}(E(u))|$ , where the sum is over integers  $u \equiv 1 \pmod{4}$ ,  $|u| \leq T$ , satisfying  $(*)$  and  $L(E(u), 1) \neq 0$ , and  $T^*$  denotes the number of terms in the sum. Similarly, let  $N_i^{**}(T) := \frac{1}{T_i^{**}} \sum |\mathbb{W}(E_i(u))|$ , where  $i = 1, 2$ , and the sum is over integers  $u \equiv 1 \pmod{4}$ ,  $|u| \leq T$ , satisfying  $(**)$  and  $L(E(u), 1) \neq 0$ , and  $T_i^{**}$  denotes the number of terms in the sum. Let  $f(T) := \frac{M^*(T)}{T^{1/2}}$ , and  $g_i(T) := \frac{N_i^{**}(T)}{T^{1/2}}$ . We obtain the following pictures

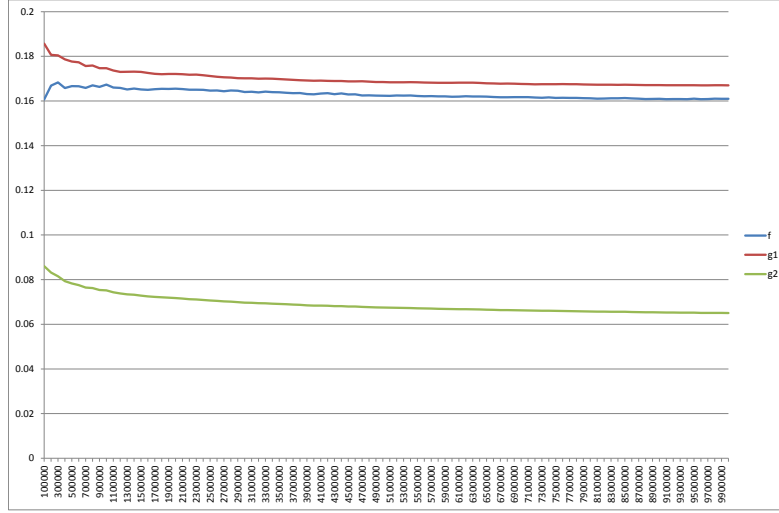


Figure 5: Graphs of the functions  $f(T)$  and  $g_i(T)$ ,  $i = 1, 2$ .

Note similarity with the predictions by Delaunay [11] for the case of quadratic twists of a given elliptic curve (and numerical evidence in [7] [8]).

## 6.2 The rank one case

Let  $T(X) := \frac{2}{X^*} \sum \frac{L'(E_1(u), 1)}{\Omega_{E_1(u)}}$ , where the sum is over integers  $u \equiv 1 \pmod{4}$ ,  $|u| \leq X$ , such that  $u^2 + 64 = p_1 \cdots p_k$  is a product of even number of different primes, and  $X^*$  denotes the number of terms in the sum. Let  $u(X) := \frac{T(X)}{X^{1/2} \log(X)}$ . Then, using PARI/GP for computations of  $L'(E_1(u), 1)$ , we obtain the following picture

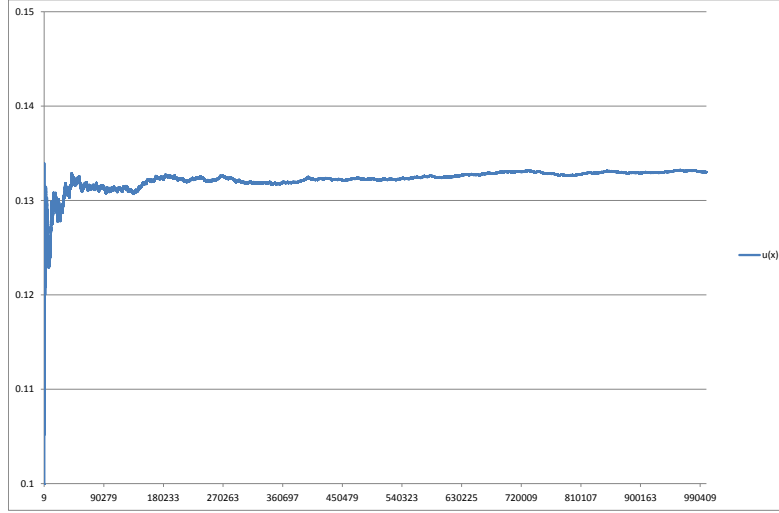


Figure 6: Graph of the function  $u(X)$ .

Hence, assuming the exact Birch and Swinnerton-Dyer conjecture for the rank one families  $E_i(u)$ ,  $i = 1, 2$ , where  $u^2 + 64 = p_1 \cdots p_k$  is a product of even number of different primes, we expect the asymptotic formulae

$$\frac{1}{X^*} \sum |\mathbb{W}(E_i(u))| R(E_i(u)) \sim c_i X^{1/2} \log X, \quad \text{as } X \rightarrow \infty,$$

where we sum over  $|u| \leq X$ ,  $u \equiv 1 \pmod{4}$ , such that  $u^2 + 64 = p_1 \cdots p_k$  is a product of even number of different primes (compare [7], section 7.2).

**Remark.** Delaunay and Roblot [13] investigated regulators of elliptic curves with rank one in some families of quadratic twists of a fixed elliptic curve, and formulated some conjectures on the average size of these regulators. Delaunay asked us to do similar calculations for our family  $E_i(u)$ . We hope to consider such investigations in some future.

## 7 Distributions of $L(E(u), 1)$ and $|\mathbb{W}(E(u))|$

### 7.1 Distribution of $L(E(u), 1)$

It is a classical result (due to Selberg) that the values of  $\log |\zeta(\frac{1}{2} + it)|$  follow a normal distribution.

Let  $E$  be any elliptic curve defined over  $\mathbb{Q}$ . Let  $\mathcal{E}$  denote the set of all fundamental discriminants  $d$  with  $(d, 2N_E) = 1$  and  $\epsilon_E(d) = \epsilon_E \chi_d(-N_E) = 1$ , where  $\epsilon_E$  is the root number of  $E$  and  $\chi_d = (d/\cdot)$ . Keating and Snaith [18]

have conjectured that, for  $d \in \mathcal{E}$ , the quantity  $\log L(E_d, 1)$  has a normal distribution with mean  $-\frac{1}{2} \log \log |d|$  and variance  $\log \log |d|$ ; see [6] [7] [8] for numerical data towards this conjecture.

Below we consider the family of Neumann-Setzer type elliptic curves. Our data suggest that the values  $\log L(E(u), 1)$  also follow an approximate normal distribution. Let  $B = 10^7$ ,  $W = \{|u| \leq B : u \equiv 1 \pmod{4} \text{ and satisfies } (**)\}$  and  $I_x = [x, x+0.1)$  for  $x \in \{-10, -9.9, -9.8, \dots, 10\}$ . We create a histogram with bins  $I_x$  from the data  $\left\{ \left( \log L(E(u), 1) + \frac{1}{2} \log \log |u| \right) / \sqrt{\log \log |u|} : |u| \in W \right\}$ . Below we picture this histogram.

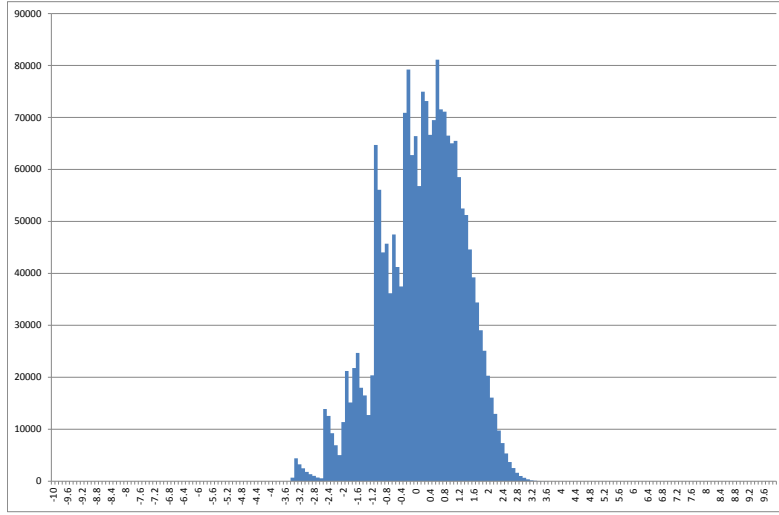


Figure 7: Histogram of values  $(\log L(E(u), 1) + \frac{1}{2} \log \log |u|) / \sqrt{\log \log |u|}$  for  $|u| \leq B : u \equiv 1 \pmod{4}$  satisfying (\*\*), and such that  $L(E, 1) \neq 0$ .

## 7.2 Distribution of $|\mathbb{W}(E(u))|$

It is an interesting question to find results (or at least a conjecture) on distribution of the order of the Tate-Shafarevich group for rank zero Neumann-Setzer type elliptic curves  $E_1(u)$  and  $E_2(u)$ . It turns out that the values of  $\log(|\mathbb{W}(E_i(u))|/\sqrt{|u|})$  are the natural ones to consider (compare Conjecture 1 in [24], and numerical experiments in [7] [8]). Below we create histograms from the data  $\left\{ \left( \log(|\mathbb{W}(E_i(u))|/\sqrt{|u|}) - \mu_i \log \log |u| \right) / \sqrt{\sigma_i^2 \log \log |u|} : |u| \in W \right\}$ , where  $\mu_1 = -\frac{1}{2}$ ,  $\mu_2 = -\frac{1}{2} - \log 2$ ,  $\sigma_1^2 = 1$ , and  $\sigma_2^2 = 1 + (\log 2)^2$  (here we use Lemma 1(iii) above, and Lemma 4 in [24]). Our data suggest that the values  $\log(|\mathbb{W}(E_i(u))|/\sqrt{|u|})$  also follow an approximate normal distribution. Below we picture these histograms.

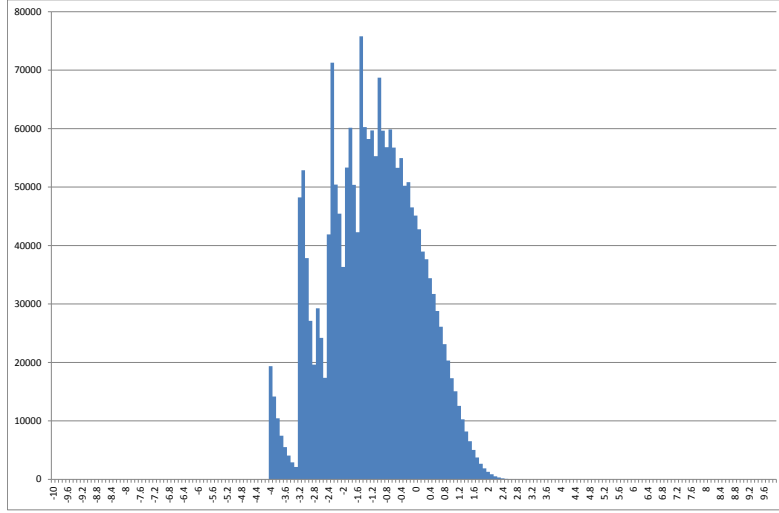


Figure 8: Histogram of values  $\left(\log(|\mathbb{W}(E_1(u))|/\sqrt{|u|}) + \frac{1}{2} \log \log |u|\right) / \sqrt{\log \log |u|}$  for  $|u| \leq B : u \equiv 1 \pmod{4}$  satisfying (\*\*), and such that  $L(E, 1) \neq 0$ .

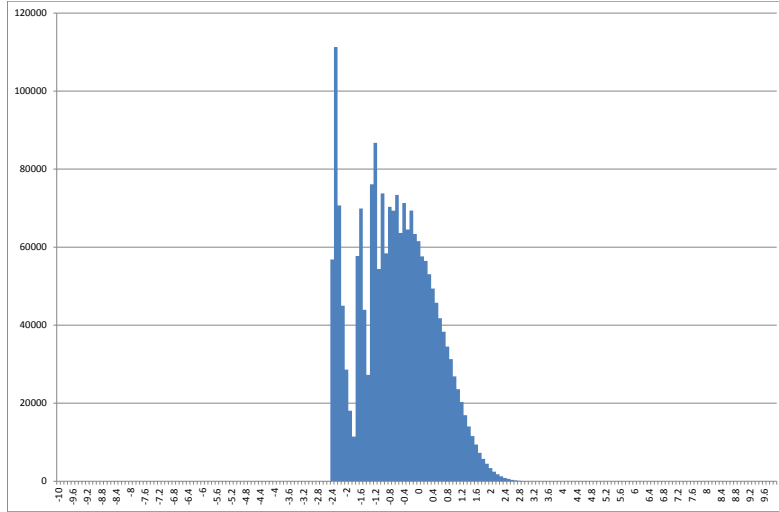


Figure 9: Histogram of values  $\left(\log(|\mathbb{W}(E_2(u))|/\sqrt{|u|}) + \left(\frac{1}{2} + \log 2\right) \log \log |u|\right) / \sqrt{(1 + (\log 2)^2) \log \log |u|}$  for  $|u| \leq B : u \equiv 1 \pmod{4}$  satisfying (\*\*), and such that  $L(E, 1) \neq 0$ .

## References

- [1] M. Bhargava, Ch. Skinner, W. Zhang, *A majority of elliptic curves over  $\mathbb{Q}$  satisfy the Birch and Swinnerton-Dyer conjecture*, [arxiv.org/abs/1407.1826](https://arxiv.org/abs/1407.1826)

- [2] J. Coates, *Lectures on the Birch-Swinnerton-Dyer Conjecture*, Notices of the ICCM **1** (2013), 29-46
- [3] J. Coates, Y. Li, Y. Tian, S. Zhai, *Quadratic twists of elliptic curves*, Proc. London Math. Soc. **110** (2015), 357-394
- [4] J. Coates, A. Wiles, *On the conjecture of Birch and Swinnerton-Dyer*, Invent. Math. **39** (1977), 223-251
- [5] J. B. Conrey, D. W. Farmer, J. P. Keating, M. O. Rubinstein and N. C. Snaith, *Integral moments of  $L$ -functions*, Proc. London Math. Soc. **91** (2005), 33-104
- [6] J. B. Conrey, J. P. Keating, M. O. Rubinstein and N. C. Snaith, *Random matrix theory and the Fourier coefficients of half-integral weight forms*, Experiment. Math. **15** (2006), 67-82
- [7] A. Dąbrowski, T. Jędrzejak, L. Szymaszkiewicz, *Behaviour of the order of Tate-Shafarevich groups for the quadratic twists of  $X_0(49)$* , In: Elliptic Curves, Modular Forms and Iwasawa Theory (in honour of John Coates' 70th birthday), Springer Proceedings in Mathematics and Statistics **188** (2016)
- [8] A. Dąbrowski, L. Szymaszkiewicz, *Behaviour of the order of Tate-Shafarevich groups for the quadratic twists of elliptic curves*, arXiv:1611.07840 [math.NT] 23 Nov 2016
- [9] A. Dąbrowski, M. Wodzicki, *Elliptic curves with large analytic order of  $\mathfrak{W}(E)$* , In: Algebra, Arithmetic and Geometry (in honour of Yu.I. Manin, vol. I), Progress in Math. **269** (2009), 407-421
- [10] H. Darmon, L. Merel, *Winding quotients and some variants of Fermat's Last Theorem*, J. reine angew. Math. **490** (1997) 81-100
- [11] C. Delaunay, *Moments of the orders of Tate-Shafarevich groups*, Int. J. Number Theory **1** (2005), 243-264
- [12] C. Delaunay, *Heuristics on class groups and on Tate-Shafarevich groups: the magic of the Cohen-Lenstra heuristics*. In: Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Ser. **341** (2007), 323-340
- [13] C. Delaunay, X.-F. Roblot, *Regulators of rank one quadratic twists*, J. Théorie Nombres Bordeaux **20** (2008), 601-624



- [14] C. Delaunay, M. Watkins, *The powers of logarithm for quadratic twists*. In: Ranks of elliptic curves and random matrix theory, London Math. Soc. Lecture Ser. **341** (2007), 189-193
- [15] C. Delaunay, C. Wuthrich, *Some remarks on self-points on elliptic curves*, Actes de la Conférence "Fonctions  $L$  et Arithmétique", 69-84, Publ. Math. Besancon Algèbre Théorie Nr., Lab. Math. Besancon, Besancon, 2010
- [16] C. D. Gonzalez-Avilés, *On the conjecture of Birch and Swinnerton-Dyer*, Trans. Amer. Math. Soc. **349** (1997), 4181-4200
- [17] B. Gross, D. Zagier, *Heegner points and derivatives of  $L$ -series*, Invent. Math. **84** (1986), 225-320
- [18] J. P. Keating, N. C. Snaith, *Random matrix theory and  $\zeta(1/2 + it)$* , Comm. Math. Phys. **214**(1) (2000), 57-89
- [19] V. Kolyvagin, *Finiteness of  $E(\mathbb{Q})$  and  $\mathbb{W}(E)$  for a class of Weil curves*, Math. USSR Izv. **32** (1989), 523-541
- [20] R. L. Miller, *Empirical evidence for the Birch and Swinnerton-Dyer conjecture*, PhD thesis, University of Washington, 2010
- [21] O. Neumann, *Elliptische Kurven mit vorgeschriebenem Reduktionsverhalten. I, II*, Math. Nachr. **49** (1971), 107-123; **56** (1973), 269-280
- [22] J. Park, B. Poonen, J. Voight, M. M. Wood, *A heuristic for boundedness of ranks of elliptic curves*, [www-math.mit.edu/~poonen/papers/bounded-ranks.pdf](http://www.math.mit.edu/~poonen/papers/bounded-ranks.pdf)
- [23] The PARI Group, PARI/GP version 2.7.2, Bordeaux, 2014, <http://pari.math.u-bordeaux.fr/>
- [24] M. Radziwiłł, K. Soundararajan, *Moments and distribution of central  $L$ -values of quadratic twists of elliptic curves*, Invent. Math. **202** (2015), 1029-1068
- [25] K. Rubin, *Tate-Shafarevich groups and  $L$ -functions of elliptic curves with complex multiplication*, Invent. Math. **89** (1987), 527-560
- [26] J.-P. Serre, *Propriétés galoisiennes des points d'ordre fini des courbes elliptiques*, Invent. Math. **15** (1972), 259-331

- [27] J.-P. Serre, *Travaux de Wiles (et Taylor,...). I*, Astérisque **237** (1996), 319-332
- [28] B. Setzer, *Elliptic curves of prime conductor*, J. London Math. Soc. (2) **10** (1975), 367-378
- [29] J. H. Silverman, *The Arithmetic of Elliptic Curves*. Second Edition, Springer 2009
- [30] Ch. Skinner, E. Urban, *The Iwasawa main conjectures for  $GL_2$* , Invent. Math. **195** (2014), 1-277
- [31] C. Soh, *Explicit methods for the Birch and Swinnerton-Dyer conjecture*, MSc Thesis, University of Oxford, 2014
- [32] W. Stein, M. Watkins, *Modular parametrizations of Neumann-Setzer elliptic curves*, Int. Math. Res. Not. **27** (2004), 1395-1405
- [33] M. Watkins, *Some heuristics about elliptic curves*, Experiment. Math. **17** (2008), 105-125
- [34] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. Math. **141** (1995), 443-551
- [35] D. Zywinia, *On the surjectivity of mod  $l$  representations associated to elliptic curves*, arXiv:1508.07661v1 [math.NT] 31 Aug 2015

Institute of Mathematics, University of Szczecin, Wielkopolska 15, 70-451 Szczecin, Poland; E-mail addresses: dabrowsk@wmf.univ.szczecin.pl and dabrowskiandrzej7@gmail.com; lucjansz@gmail.com